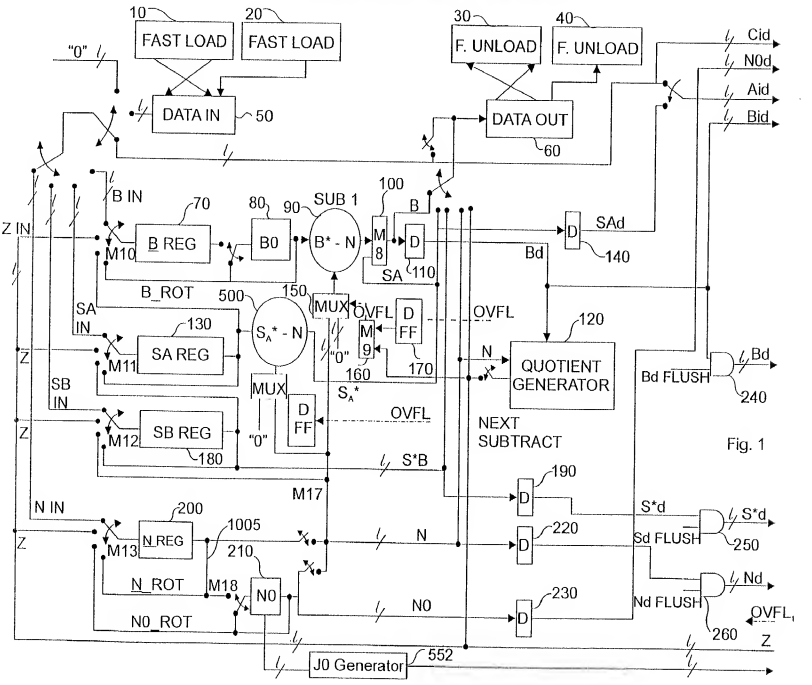

Fig. 1

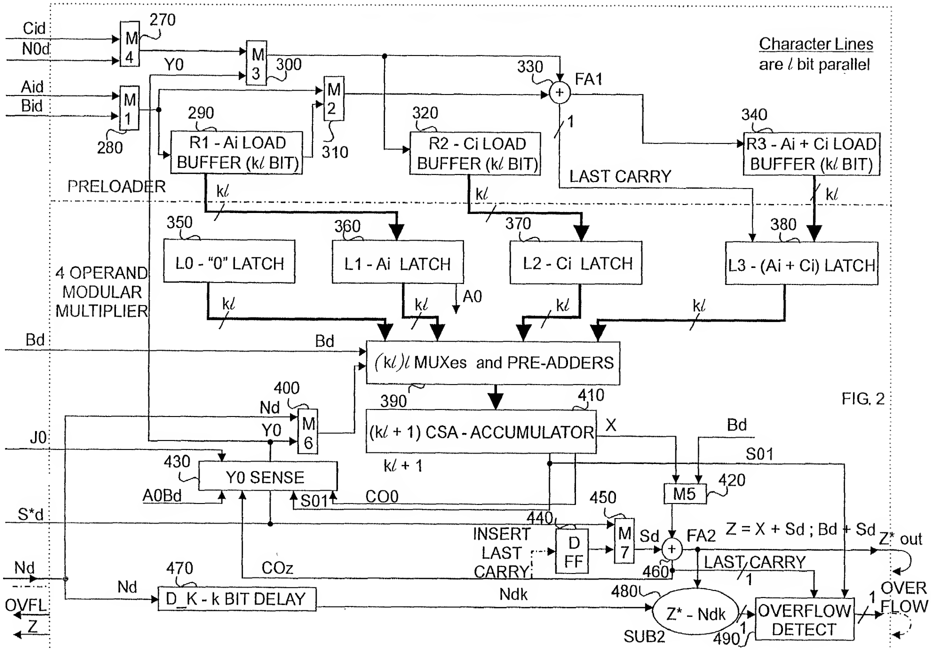
Cid
N0d
Aid
Bid
M 4
270
M 1
280
M 3
300
Y0
M 2
310
R1 - Ai LOAD BUFFER (kℓ BIT)
290
R2 - Ci LOAD BUFFER (kℓ BIT)
320
330
FA1
1
LAST CARRY
R3 - Ai + Ci LOAD BUFFER (kℓ BIT)
340
Character Lines are ℓ bit parallel
PRELOADER
kℓ
4 OPERAND MODULAR MULTIPLIER
L0 - "0" LATCH
350
L1 - Ai LATCH
360
A0
L2 - Ci LATCH
370
L3 - (Ai + Ci) LATCH
380
Bd
(kℓ)ℓ MUXes and PRE-ADDERS
390
(kℓ + 1) CSA - ACCUMULATOR
410
kℓ + 1
X
J0
Nd
Y0
M 6
400
Y0 SENSE
430
A0Bd
S01
CO0
S*d
COz
Nd
D_K - k BIT DELAY
470
Ndk
INSERT LAST CARRY
D FF
440
M 7
450
Sd
M5
420
S01
FA2
460
Z = X + Sd ; Bd + Sd
Z* out
LAST CARRY
Z* - Ndk
480
SUB2
490
OVERFLOW DETECT
OVER FLOW
OVFL
Z

FIG. 2

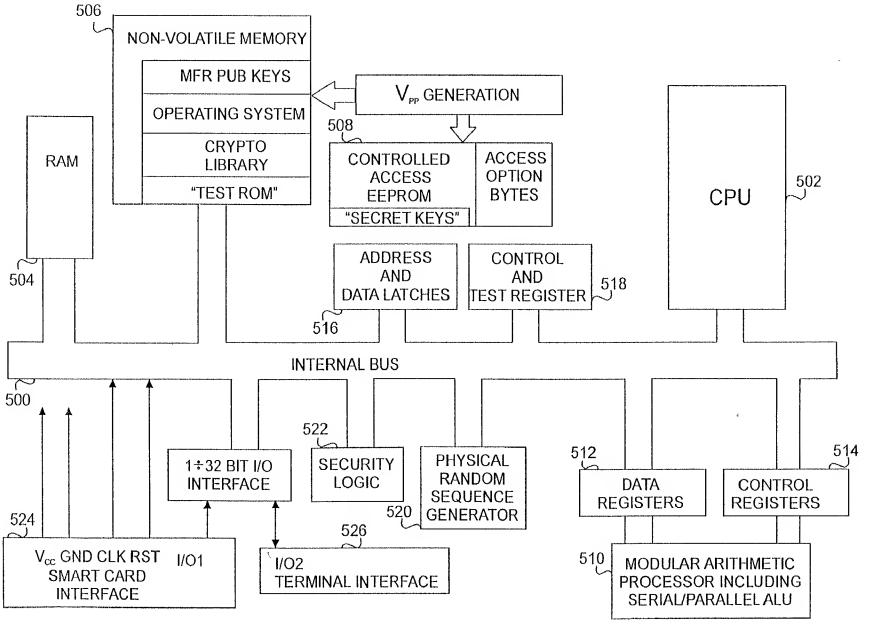

FIG. 3

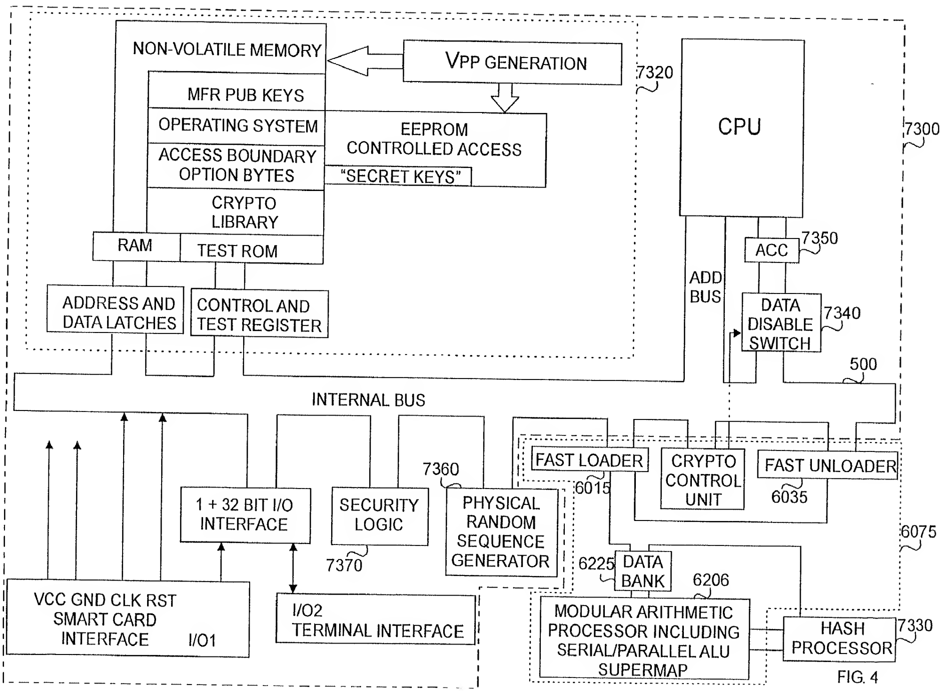

FIG. 4

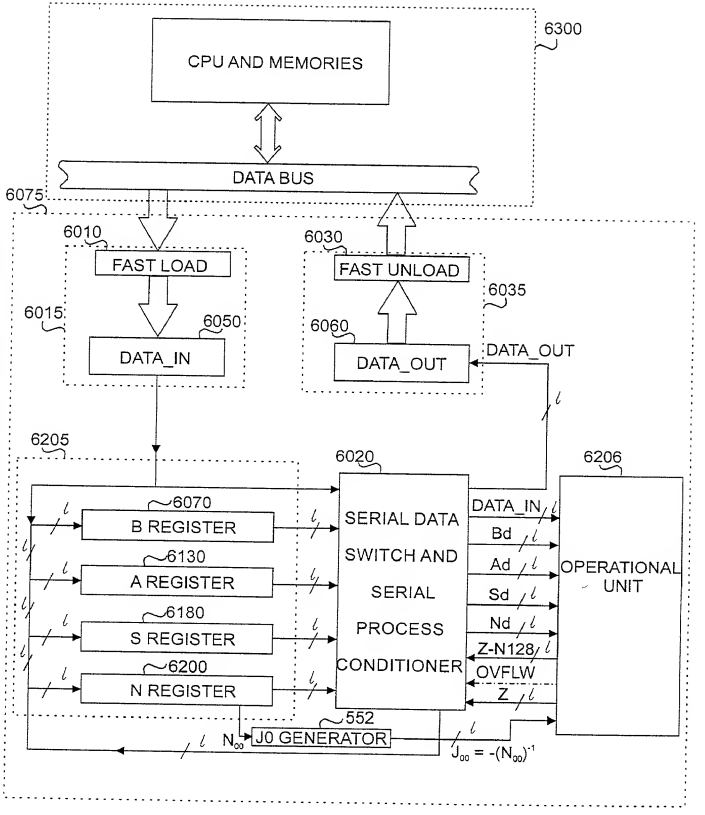
6300
CPU AND MEMORIES
DATA BUS
6075
6010
FAST LOAD
6015
6050
DATA_IN
6030
FAST UNLOAD
6035
6060
DATA_OUT
DATA_OUT
6205
6020
6206
6070
B REGISTER
6130
A REGISTER
6180
S REGISTER
6200
N REGISTER
SERIAL DATA SWITCH AND SERIAL PROCESS CONDITIONER
DATA_IN
Bd
Ad
Sd
Nd
Z-N128
OVFLW
Z
OPERATIONAL UNIT
552
J0 GENERATOR
N_{00}
$J_{00} = -(N_{00})^{-1}$

FIG. 5

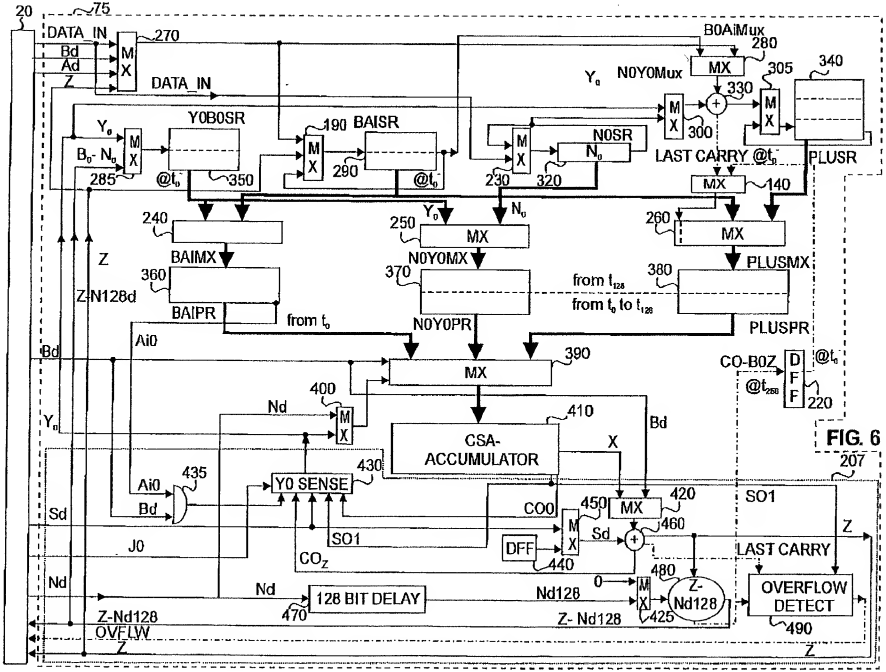
20
75
DATA_IN
Bd
Ad
Z
MX
270
DATA_IN
B0AiMux
280
MX
Y0
N0Y0Mux
330
305
340
MX
300
Y0B0SR
190
BAISR
N0SR
N0
B0- N0
285
@t0
350
290
@t0
230
320
LAST CARRY @t0
PLUSR
MX
140
240
250
Y0
N0
260
MX
MX
BAIMX
N0Y0MX
PLUSMX
Z
360
370
380
from t128
from t0 to t128
Z-N128d
BAIPR
from t0
N0Y0PR
PLUSPR
Ai0
Bd
390
MX
CO-B0Z
@t0
DFF
@t256
220
400
Nd
410
Y0
Bd
CSA-
ACCUMULATOR
X
207
430
435
Ai0
Y0 SENSE
SO1
Bd
CO0
450
MX
420
Sd
460
Z
Sd
J0
SO1
DFF
LAST CARRY
COZ
440
480
0
Nd
Nd
128 BIT DELAY
Nd128
Z-Nd128
OVERFLOW
DETECT
470
425
490
Z-Nd128
Z- Nd128
OVFLW
Z
Z

FIG. 6

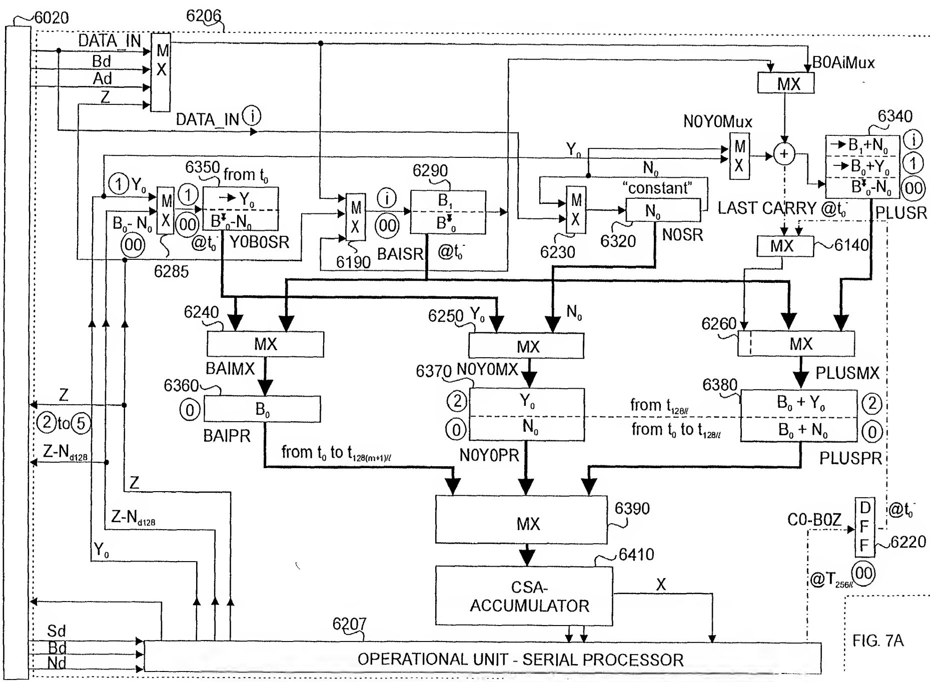
6020
6206
DATA_IN
Bd
Ad
Z
MX
DATA_IN (i)
B0AiMux
MX
N0Y0Mux
MX
6340
→B1+N0 (i)
→B0+Y0 (1)
B0-N0 (00)
PLUSR
Y0
N0
"constant"
N0
N0SR
6320
6230
LAST CARRY @t0-
MX
6140
6290
B1
B0
BAISR
@t0-
6190
(i)
(00)
6350 from t0
→Y0
B0-N0
Y0B0SR
(1) Y0
B0- N0
(00)
@t0-
6285
6240
MX
BAIMX
6360
B0
BAIPR
6250 Y0
N0
MX
6370 N0Y0MX
Y0
N0
N0Y0PR
6260
MX
PLUSMX
6380
B0 + Y0
B0 + N0
PLUSPR
from t128//
from t0 to t128//
from t0 to t128(m+1)//
6390
MX
6410
CSA-ACCUMULATOR
X
Z
(2)to(5)
Z-Nd128
Z
Z-Nd128
Y0
C0-B0Z
DFF
@t0-
6220
@T256// (00)
Sd
Bd
Nd
6207
OPERATIONAL UNIT - SERIAL PROCESSOR

FIG. 7A

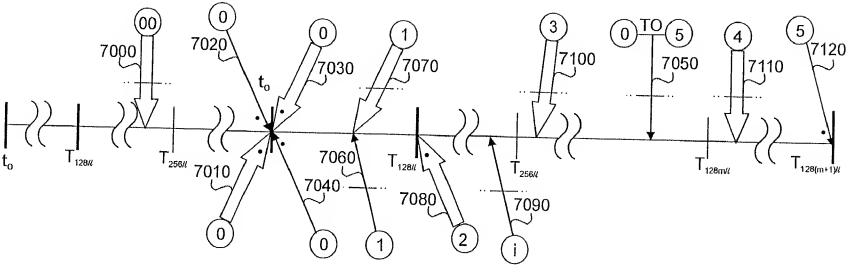

FIG. 7B

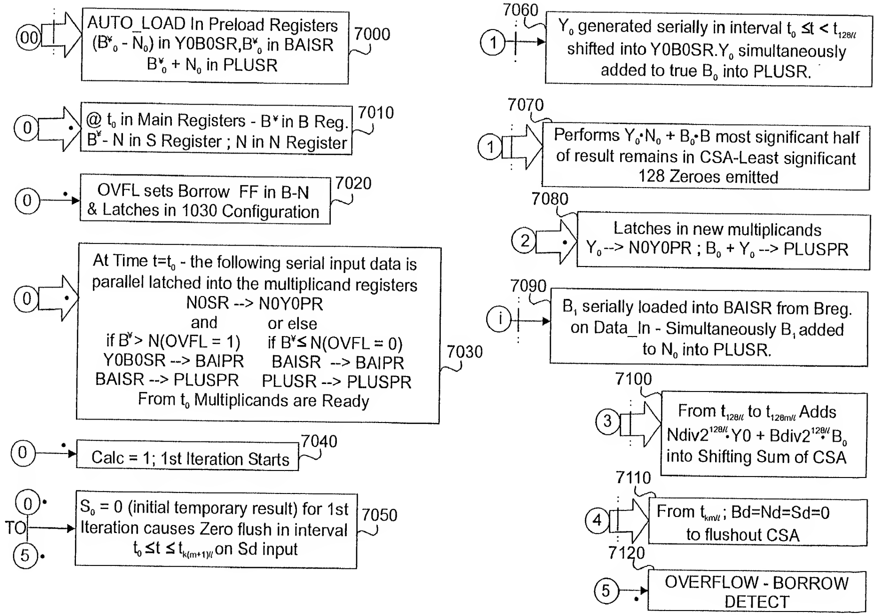
00
AUTO_LOAD In Preload Registers
(B¥0 - N0) in Y0B0SR,B¥0 in BAISR
B¥0 + N0 in PLUSR
7000
0
@ t0 in Main Registers - B¥ in B Reg.
B¥- N in S Register ; N in N Register
7010
0
OVFL sets Borrow FF in B-N
& Latches in 1030 Configuration
7020
0
At Time t=t0 - the following serial input data is
parallel latched into the multiplicand registers
N0SR --> N0Y0PR
and
if B¥ > N(OVFL = 1)
Y0B0SR --> BAIPR
BAISR --> PLUSPR
or else
if B¥ ≤ N(OVFL = 0)
BAISR --> BAIPR
PLUSR --> PLUSPR
From t0 Multiplicands are Ready
7030
0
Calc = 1; 1st Iteration Starts
7040
0
TO
5
S0 = 0 (initial temporary result) for 1st
Iteration causes Zero flush in interval
t0 ≤t ≤ tk(m+1)ℓ on Sd input
7050
7060
1
Y0 generated serially in interval t0 ≤t < t128ℓ
shifted into Y0B0SR.Y0 simultaneously
added to true B0 into PLUSR.
7070
1
Performs Y0•N0 + B0•B most significant half
of result remains in CSA-Least significant
128 Zeroes emitted
7080
2
Latches in new multiplicands
Y0--> N0Y0PR ; B0 + Y0 --> PLUSPR
7090
i
B1 serially loaded into BAISR from Breg.
on Data_In - Simultaneously B1 added
to N0 into PLUSR.
7100
3
From t128ℓ to t128mℓ Adds
Ndiv2^128ℓ•Y0 + Bdiv2^128ℓ•B0
into Shifting Sum of CSA
7110
4
From tkmℓ ; Bd=Nd=Sd=0
to flushout CSA
7120
5
OVERFLOW - BORROW
DETECT

FIG. 7C

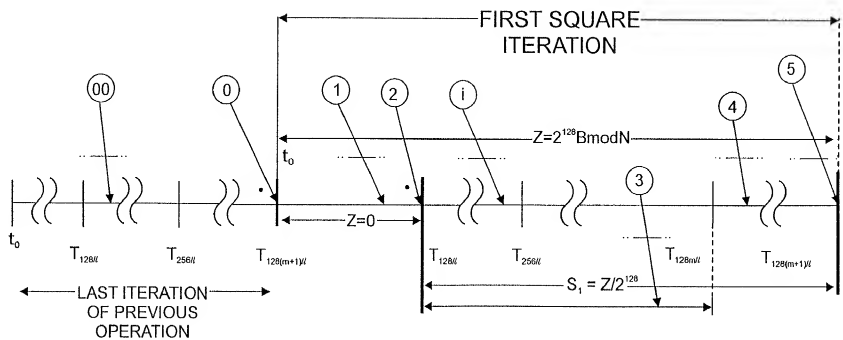
FIRST SQUARE ITERATION
00
0
1
2
i
3
4
5
Z=2^128BmodN
t_0
t_0
Z=0
$T_{128/l}$
$T_{256/l}$
$T_{128(m+1)/l}$
$T_{128/l}$
$T_{256/l}$
$T_{128m/l}$
$T_{128(m+1)/l}$
$S_1 = Z/2^{128}$
LAST ITERATION OF PREVIOUS OPERATION

FIG. 7D

	N_0	N_0^{-1}	$-(N_0^{-1})$
1	0001	0001	1111
3	0011	1011	0101
5	0101	1101	0011
7	0111	0111	1001
9	1001	1001	0111
11	1011	0011	1101
13	1101	0101	1011
15	1111	1111	0001

$\mathcal{S} = 1$
GF(p)
$\ell = 4$

	N_0	$-N_0^{-1} = N_0^{-1}$
1	0001	0001
3	0011	1111
5	0101	0101
7	0111	1011
9	1001	1001
11	1011	0111
13	1101	1101
15	1111	0011

$\mathcal{S} = 0$
No Carry
GF(2^s)
$\ell = 4$

$\mathcal{S} = 1$
GF(p)
$\ell = 2$

N_0	N_0^{-1}	$-N_0^{-1}$
01	01	11
11	11	01

N_0	N_0^{-1}
01	01
11	11

$\mathcal{S} = 0$
No Carry
GF(2^s)
$\ell = 2$

FIG. 8A

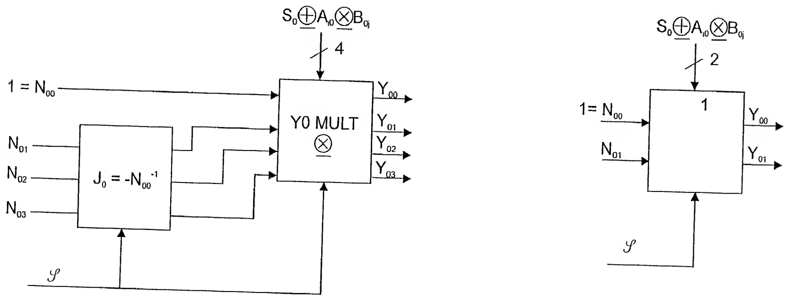
$S_0 \oplus A_{i0} \otimes B_{0j}$
4
$1 = N_{00}$
N_{01}
N_{02}
N_{03}
$J_0 = -N_{00}^{-1}$
Y0 MULT
$\otimes$
Y_{00}
Y_{01}
Y_{02}
Y_{03}
$\mathcal{S}$
$S_0 \oplus A_{i0} \otimes B_{0j}$
2
1
$1 = N_{00}$
N_{01}
Y_{00}
Y_{01}
$\mathcal{S}$

FIG. 8B